To NHCNE beneficiaries notified by letter of possible loss of Personal Identifiable Information (PII) in Pensacola, Florida, please read the following information carefully. While there is no evidence to suggest personal data has been compromised, we take this situation very seriously and continue to strive to protect and secure your PII. The data lost is limited to patient name and sponsor's social security number: No medical information was compromised.

The course of action for affected beneficiaries is to monitor their financial statements for suspicious activity. If any unusual activity is noted, the steps for reporting such activity are listed in the Frequently Asked Questions below.

We regret this unfortunate development and any inconvenience caused by this data loss in Pensacola. We will continue to monitor the situation. Should you have further questions or concerns, please contact 1-866-284-4282 and speak with a PII Incident Response Line representative from 0800-1630, Monday through Friday.

Possible Loss of Personally Identifiable Information (PII)

On October 19, 2009, a computer disk (CD) containing PII was reported missing from Naval Hospital Pensacola (NHP), Florida. The information on the CD consisted of a staff member's working files for Population Health compiled at Naval Health Clinic New England (NHCNE) from October 2005-July 2009. The CD was hand carried to NHP by the transferring staff member and subsequently lost. The CD contained data files used to track notifications for annual health screenings. While there is no evidence to suggest personal data has been misused, it is recommended that everyone carefully monitor bank statements, credit card statements and other financial transactions for suspicious activity. Those affected will be notified by letter detailing the incident.

Frequently Asked Questions

1. How can I tell if my information was compromised?

At this point there is no evidence that any missing data has been used illegally. However, the Department of Navy is asking each individual to be extra vigilant and to carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved.

2. What is the earliest date at which suspicious activity might have occurred?

The CD was last seen on October 13, 2009, and is presumed lost. If data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that individuals may notice suspicious activity beginning in the middle of October.

3. I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent

being victimized by credit card fraud or identity theft?

The Department of Navy strongly recommends that individuals closely monitor their financial statements and visit www.ftc.gov/bcp/edu/microsites/idtheft

4. Should I reach out to my financial institutions or will the Department of Navy do this for me?

The Department of Navy does not believe that it is necessary to contact financial institutions or contact credit cards and bank accounts, unless you detect suspicious activity.

5. Where should I report suspicious or unusual activity?

The Federal Trade Commission recommends the following four steps if you detect suspicious activity:

Step 1- Contact the fraud department of one of the following three major credit bureaus:
Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.
Experian: 1-800-680-7289; www.experian.com P.O. Box 9532 Allen, TX 75013.
TransUnion: 1800-680-7289; www.transunion.com Fraud Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

Step 2- Close any accounts that have been tampered with or opened fraudulently.

Step 3- File a police report with your local police or the police in the community where the identity theft took place.

Step 4- File a complaint with the Federal Trade Commission by using the FTC's Identity Theft Hotline by phone: 1-877-438-4338, online at www.ftc.gov/bcp/edu/microsites/idtheft , or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington DC 20580.

6. I know that the Department of Navy maintains my health records electronically. Was the information also compromised?

No electronic medical records were compromised. The data lost is limited to patient's name, date of birth, and sponsor's social security number. This information was used to send out notifications for annual health screenings. However, this information could still be of potential use to identify thieves and we recommend that all patients be extra vigilant in monitoring for signs of potential identity or misuse of this information.

7. What is being done to insure this does not happen again?

Command wide training stand down on PII labeling, encryption, incident reporting, and accountability for safeguarding of Information Technology resources. Aggressive ongoing compliance spot checks. Review of PII holdings with goal of reducing amount of PII collected. Implementation of the Data At Rest (DAR) solution for encryption.

Where can I get further, up-to-date information?

Naval Hospital Pensacola and Naval Health Clinic New England will provide any

updates via our websites and a toll-free telephone number for patients has been established. Please visit http://www.med.navy.mil/sites/pcola or http://nhcne.med.navy.mil/index.asp or call 1-866-284-4282.

We urge everyone possibly affected to be extra vigilant and monitor their financial accounts.